

# Fighting Malicious SEO Campaigns at a National Level – the Case of Brazil

Cristine Hoepers, Ph.D.  
CERT.br/NIC.br  
cristine@cert.br

Klaus Steding-Jessen, Ph.D.  
CERT.br/NIC.br  
jessen@cert.br

UE25 – Strasbourg, FR – September 1<sup>st</sup>, 2025

cert.br nic.br cgi.br



Computer Emergency Response Team Brazil

National CSIRT of Last Resort

# Services Provided to the Community

Incident Management	Situational Awareness	Knowledge Transfer
<ul style="list-style-type: none"> <li>▶ Coordination</li> <li>▶ Technical Analysis</li> <li>▶ Mitigation and Recovery Support</li> </ul>	<ul style="list-style-type: none"> <li>▶ Data Acquisition                             <ul style="list-style-type: none"> <li>▶ Distributed Honeypots</li> <li>▶ SpamPots</li> <li>▶ Threat feeds</li> </ul> </li> <li>▶ Information Sharing</li> </ul>	<ul style="list-style-type: none"> <li>▶ Awareness                             <ul style="list-style-type: none"> <li>▶ Development of Best Practices</li> <li>▶ Outreach</li> </ul> </li> <li>▶ Training</li> <li>▶ Technical and Policy Advisory</li> </ul>

## Affiliations and Partnerships:



SEI  
Partner  
Network



## Mission

To increase the level of security and incident handling capacity of the networks connected to the Internet in Brazil.

## Constituency

Any network that uses Internet Resources allocated by NIC.br

- IP addresses or ASNs allocated to Brazil
- domains under the ccTLD .br

## Governance

Maintained by **NIC.br** – The National Internet Registry (NIR)

- all activities are funded by .br domain registration

NIC.br is the **executive branch of CGI.br** – The Brazilian Internet Steering Committee

- a multistakeholder organization
- with the purpose of coordinating and integrating all Internet service initiatives in Brazil

<https://cert.br/about/>  
<https://cert.br/sobre/filiacoes/>  
<https://cert.br/about/rfc2350/>

# First let's cover some possible misconceptions

- It is NOT about sponsored ads
  - it is not ad fraud
    - there is no paid advertisement
- The objective IS NOT to deliver malware
  - it is only to be the top result on searches of interest
    - e.g. sports betting platforms
- It is only about increasing the ranking in search engines
  - compromising legitimate websites with good reputation
  - manipulating keywords and referrals

# Malicious Search Engine Optimization (SEO) Campaigns

- Compromise legitimate websites
- Include terms related to the content they want to promote
  - e.g. sports betting sites
- Include links to other compromised websites, to create cross-reference
- Only serve the “malicious” content to search engine related requests
  - indexing bots
  - users following links from search results

## Reminder:

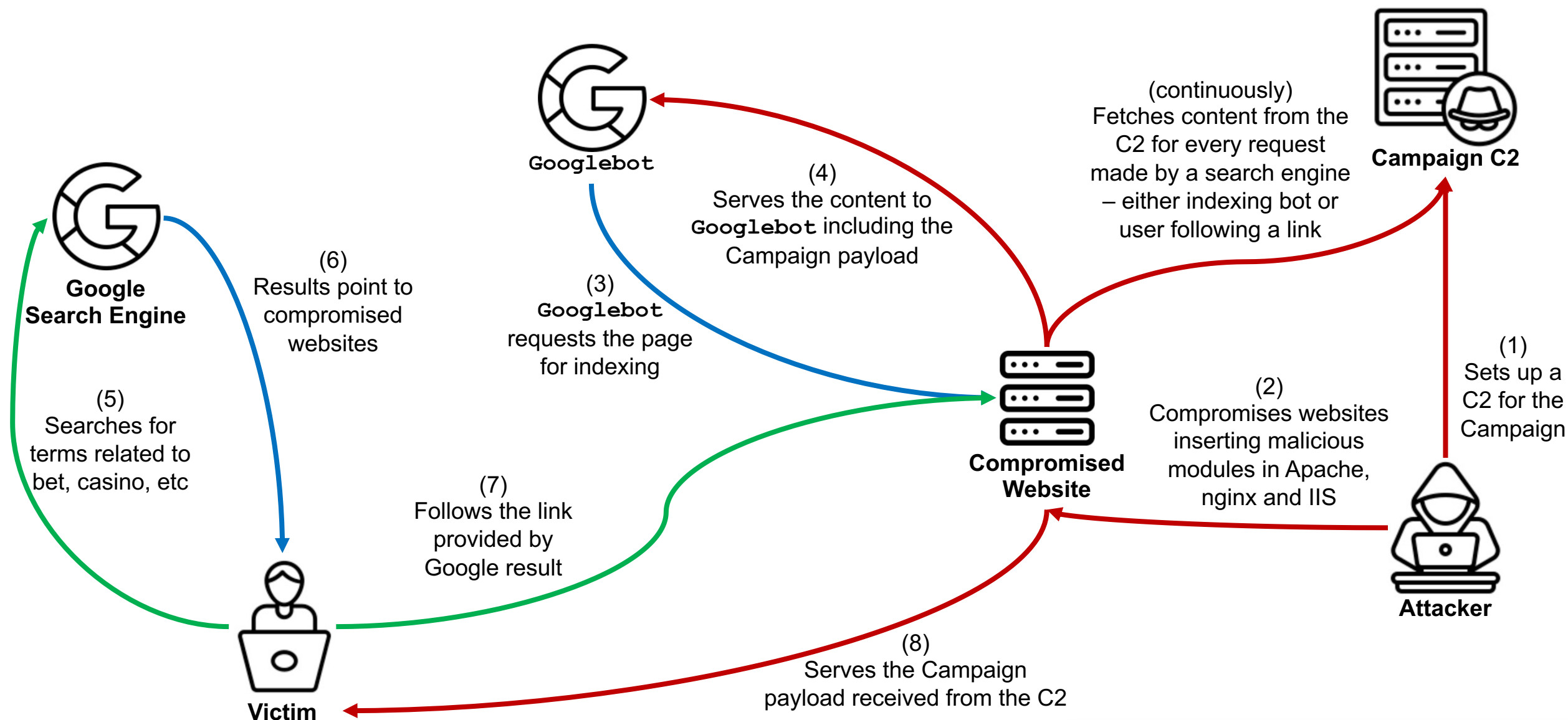
- Search Engine Optimization (SEO): the process of improving the quality and quantity of website traffic to a website or a web page from search engines.

Techniques are described by Google at:

<https://developers.google.com/search/docs/fundamentals/seo-starter-guide>

# Overview of the Attack

TLP:CLEAR





# Google Search Example

TLP:CLEAR

Google  
bet ypiranga x nautico site:.br

https://...es.gov.br > bet > ypiranga-...  
**ypiranga x nautico | Aposte já!**  
ypiranga x nautico **TigerVIP.APP** Ganhe 40R\$ ao se inscrever para jogar Ganesha Gold em nosso cassino online! Por ypiranga x nautico, da Agência Brasília | Edição ...  
66.655 respostas · Melhor resposta: ypiranga x nautico **TigerVIP.APP** Ganhe 40R\$ ao s...

https://...edu.br · 31 de mar. de 2025  
**classificações de náutico x ypiranga futebol clube**  
... de náutico x ypiranga futebol clube, Cassino online 24 ... **bet** slots online free tips champions league partidas de londrina esporte ...

https://...edu.br > video > nautico x ypiranga p...  
**nautico x ypiranga palpites**  
Acumule pontos em apostas esportivas e desbloqueie jogos exclusivos de cassino na nautico x ypiranga palpites!

https://...sp.gov.br > bet > campeonato-italiano  
**campeonato italiano**  
... ypiranga x trem YSwin Ganesha Gold ypy **bet** YSwin Jogo YSwin YSwin Fortune ...  
**nautico** yoyo casino no deposit bonus YSwin app YSwin baixar app YSwin ...


http://...am.gov.br > game > nautico x ypiranga palpites  
**nautico x ypiranga palpites**  
**nautico x ypiranga palpites**Do Brasileiro à Champions League, todas as competições em uma só plataforma. nautico x ypiranga palpites, o paraíso do apostador!


Google  
bet ypiranga x nautico site:.br

Todas Notícias Vídeos Imagens Shopping Vídeos curtos Web : Mais Ferramentas

https://...gov.br > game > nautico x ypirang...  
**nautico x ypiranga palpites**  
**nautico x ypiranga palpites!** Mais de 450 jogos de mesa com limites para todos os perfis: de R\$0,50 a R\$1.000.000 por rodada.

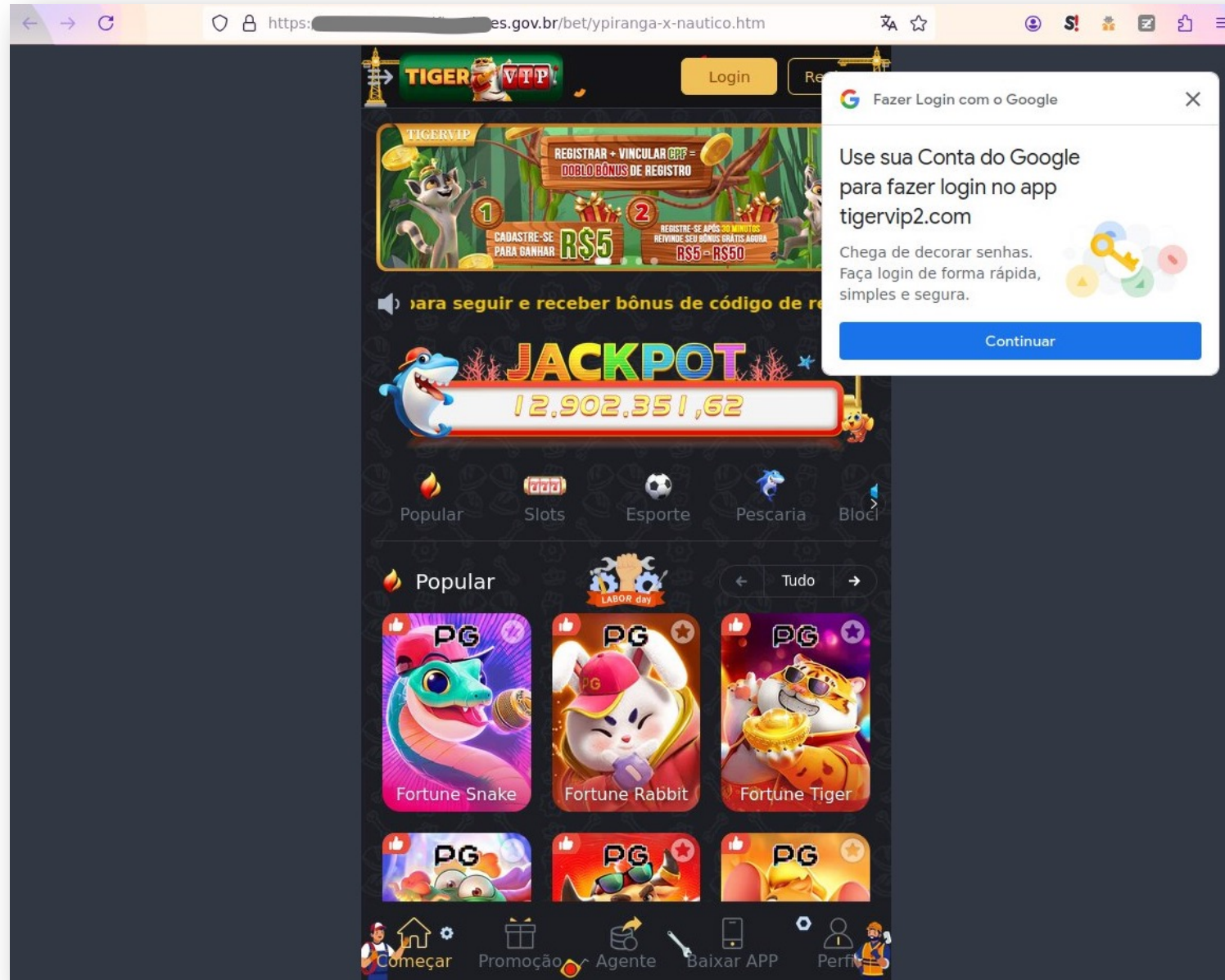
https://...edu.br > ios > nautico x ypiranga palpites  
**nautico x ypiranga palpites|AppStore1.22**  
**nautico x ypiranga palpites**,Segurança verificada por auditorias internacionais independentes. Na nautico x ypiranga palpites, transparência é compromisso!

https://...edu.br · 2 de abr. de 2025  
**nautico x ypiranga palpites\_V2.37**  
**nautico x ypiranga palpites**,Plataforma com modo econômico para conexões limitadas ... bochum x cassino rio grande bingo pop **bet** 365 directo jogar jogo da mega com ...

https://...edu.br · 1 de abr. de 2025  
**náutico x ypiranga palpites- Android App**  
**náutico x ypiranga palpites**,Líder na Ásia, agora conquistando o Brasil! Experimente nosso cassino ao vivo com dealers profissionais e HD streaming.

# Result following the first highlighted link

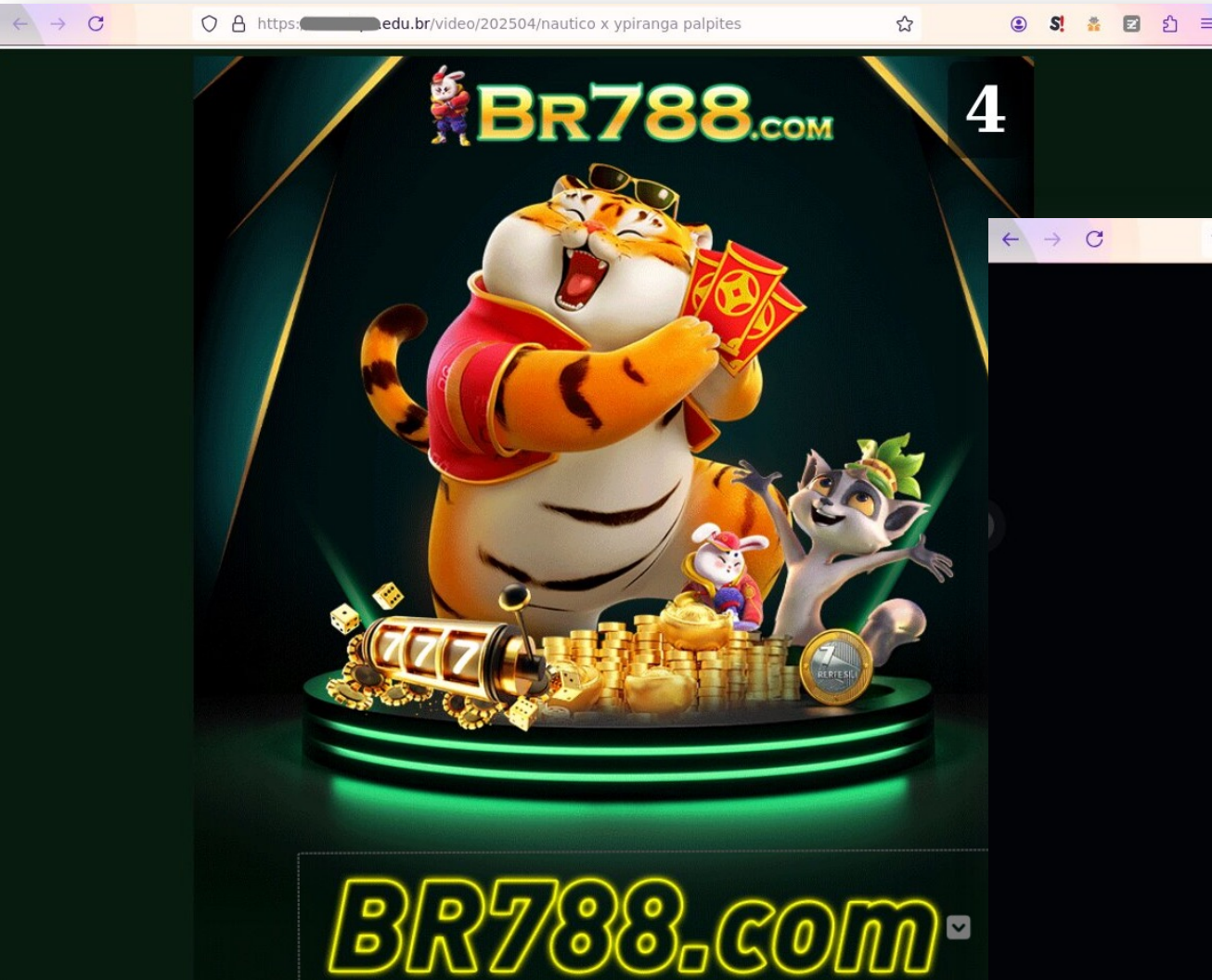
TLP:CLEAR



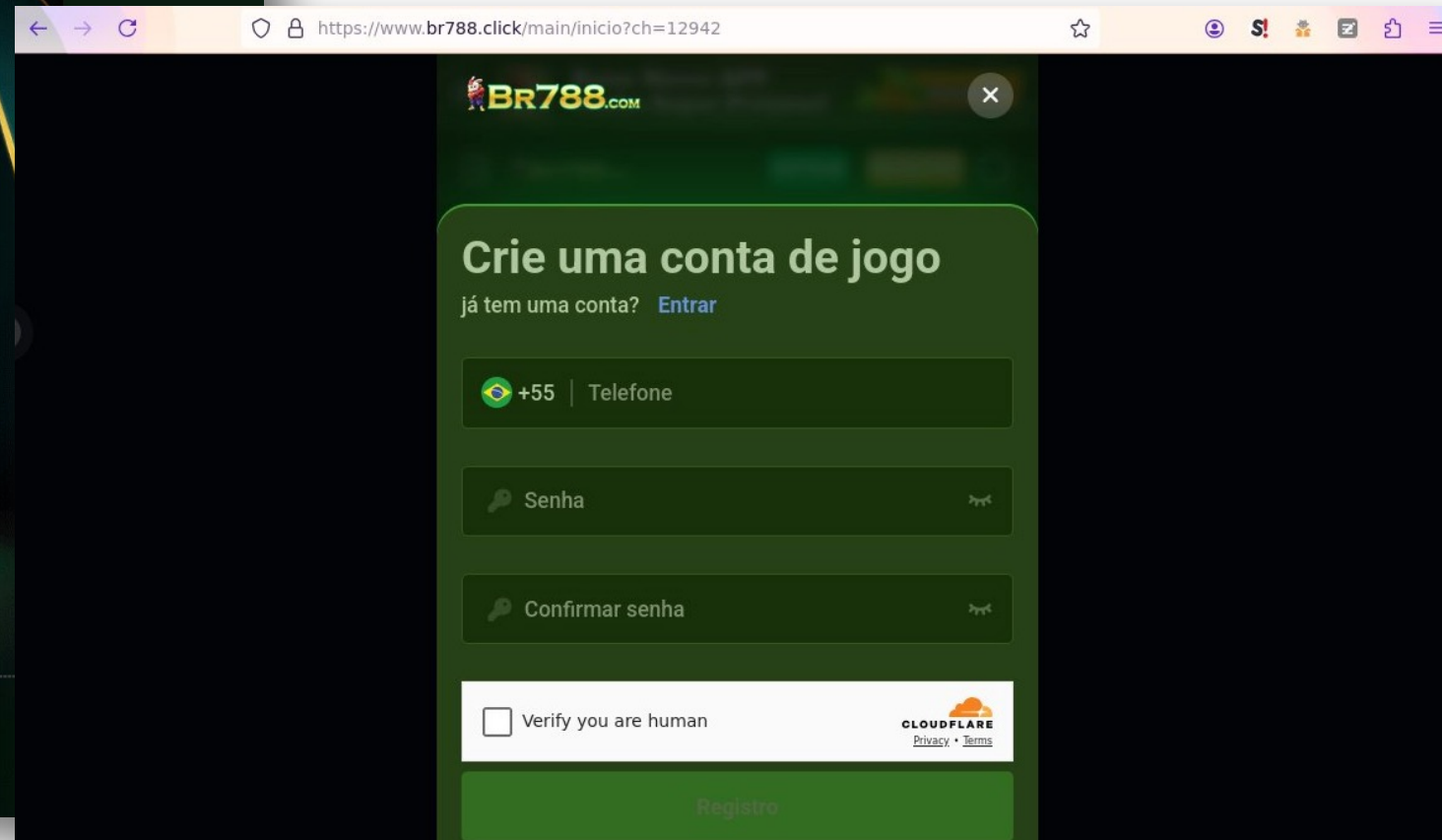


# Result following the second highlighted link

– Plays a video for 5 seconds...



– ...then redirects to the website





# Compromised site: regular view vs Googlebot view

TLP:CLEAR

```
$ curl -L -s -A Googlebot https://[victim].edu.br/
```

```
$ curl -L -s https://[victim].edu.br/
```

```
<script nonce="Ia9njl1jawc2En6k70kJwJM6">^M
window.addEventListener('DOMContentLoaded', (event) => {^M
  const loginShowing = document.querySelector('a[href$=
const leftPanel1 = document.querySelector("#recently-updated-
const leftPanel2 = document.querySelector("#recent-ac
const leftPanel3 = document.querySelector("div.activity-list"
const rightPanel = document.querySelector("div.tri-la
  if (loginShowing) {^M
    leftPanel1.style.visibility = 'visible';^M
    leftPanel2.style.visibility = 'visible';^M
    leftPanel3.style.visibility = 'visible';^M
    rightPanel.style.visibility = 'visible';^M
  }^M
});^M
</script>
<!-- End: custom user content -->

<!-- Translations for JS -->
</head>
<body
  class="tri-layout ">

  <a class="px-m py-s skip-to-content-link print-hidden" href="
<div component="notification"
  option:notification:type="success"
  option:notification:auto-hide="true"
```

```
const rightPanel = document.querySelector("div.tri-layout-right");^M
if (loginShowing) {^M
  leftPanel1.style.visibility = 'visible';^M
  leftPanel2.style.visibility = 'visible';^M
  leftPanel3.style.visibility = 'visible';^M
  rightPanel.style.visibility = 'visible';^M
}^M
});^M
</script><div class="sitemap">
<h1>Sitemaps</h1>
<div class="urls">
<a href="/ios/202505/good%20slots">good slots</a>
<a href="/ios/202505/gold%20casino%20game%20777">gold casino game 777</a>
<a href="/game/2025-05/estados%20unidos%20basquete%20jogo">estados unidos basquete jogo</a>
<a href="/app/202505/gazovik%20orenburg%20x%20cska">gazovik orenburg x cska</a>
<a href="/game/202505/cassino%20em%20cuba">cassino em cuba</a>
<a href="/video/2025-05/barcelona%20e%20real%20sociedad">barcelona e real sociedad</a>
<a href="/game/202505/macaca">macaca</a>
<a href="/android/202505/7.bet%20entrar">7.bet entrar</a>
<a href="/ios/202505/lol%20dl">lol dl</a>
<a href="/ios/202505/baixar%20lobo888">baixar lobo888</a>
<a href="/android/202505/aviator%20horarios">aviator horarios</a>
<a href="https://[redacted].br/app/2025-05/jogos%20campeonato%20brasileiro">jogos campeonato brasileiro</a>
<a href="https://[redacted].gov.br/android/202505/numeros%20da%20sorte%20para%20mega%20da%20virada%202023">numeros da
sa sorte para mega da virada 2023</a>
<a href="http://[redacted].edu.br/video/2025-05/grafico%20lobo888">grafico lobo888</a>
<a href="http://[redacted].br/video/202505/o&#039;que%20%C3%A9%20saque%20corre">o&#039;que é saque corre</a>
<a href="https://[redacted].br/static/help.jsp?ios=202505%2Fjogos%20de%20pr%C3%A9-ol%C3%ADmpico">jogos de pré-olimpico</a>
<a href="https://[redacted].edu.br/ios/202505/grupo%20telegram%20f12%20bet">grupo telegram f12 bet</a>
<a href="http://[redacted].br/sigaa/public/programa/index.jsp?android=202505%2Funo%20jogo%20online">uno
jogo online</a>
<a href="https://[redacted].edu.br/ios/202505/jogo%20rainha%20777">jogo rainha 777</a>
<a href="http://[redacted].edu.br/game/2025-05/jogos%20de%20pintar">jogos de pintar</a>
<a href="https://[redacted].com.br/android/202505/tigrinho%20estrela%20bet">tigrinho estrela bet</a>
<a href="https://[redacted].br/game/202505/in%20flames%20soundtrack%20to%20your%20escape%20torrent">in f
lames soundtrack to your escape torrent</a>
</div>
</div>
<!-- End: custom user content -->

<!-- Translations for JS -->
</head>
<body
  class="tri-layout ">
```


# Compromised site: Googlebot view explained

Section **A** is the content that will be served to visitors coming via a google search

Section **B** includes links to other compromised websites

All extra code is dynamically generated in memory

- malicious content is only served if the access comes via a search engine
- there are no permanent changes to the website source code or filesystem structure
- links and local content provided by the C2



```

    }));^M
  </script><div class="sitemap">
    <h1>Sitemaps</h1>
    <div class="urls">
      <a href="/ios/202505/good%20slots">good slots</a>
      <a href="/ios/202505/gold%20casino%20game%20777">gold casino game 777</a>
      <a href="/game/2025-05/estados%20unidos%20basquete%20jogo">estados unidos basquete jogo</a>
      <a href="/app/202505/gazovik%20orenburg%20x%20cska">gazovik orenburg x cska</a>
      <a href="/game/202505/cassino%20em%20cuba">cassino em cuba</a>
      <a href="/video/2025-05/barcelona%20e%20real%20sociedad">barcelona e real sociedad</a> ←
      <a href="/game/202505/macaca">macaca</a>
      <a href="/android/202505/7.bet%20entrar">7.bet entrar</a>
      <a href="/ios/202505/lol%20dl">lol dl</a>
      <a href="/ios/202505/baixar%20lobo888">baixar lobo888</a>
      <a href="/android/202505/aviator%20horarios">aviator horarios</a>
      <a href="https://[redacted].br/app/2025-05/jogos%20campeonato%20brasileiro">jogos campeonato brasileiro</a>
      <a href="https://[redacted].gov.br/android/202505/numeros%20da%20sorte%20para%20mega%20da%20virada%202023">numeros da
      <a href="http://[redacted].edu.br/video/2025-05/grafico%20lobo888">grafico lobo888</a>
      <a href="http://[redacted].br/video/202505/o&#039;que%20C3%A9%20saque%20corre">o&#039;que é saque corre</a>
      <a href="https://[redacted].br/static/help.jsp?ios=202505%2Fjogos%20de%20pr%C3%A9-ol%C3%ADmpico">jogos de pré-olím
      <a href="https://[redacted].edu.br/ios/202505/grupo%20telegram%20f12%20bet">grupo telegram f12 bet</a>
      <a href="http://[redacted].br/sigaa/public/programa/index.jsp?android=202505%2Funo%20jogo%20online">uno
      <a href="https://[redacted].edu.br/ios/202505/jogo%20rainha%20777">jogo rainha 777</a>
      <a href="http://[redacted].edu.br/game/2025-05/jogos%20de%20pintar">jogos de pintar</a>
      <a href="https://[redacted].com.br/android/202505/tigrinho%20estrela%20bet">tigrinho estrela bet</a>
      <a href="https://[redacted].br/game/202505/in%20flames%20soundtrack%20to%20your%20escape%20torrent">in f
      </div>
    </div>
    <!-- End: custom user content -->

    <!-- Translations for JS -->
  </head>
  <body
    class="tri-layout ">
  
```

# Compromised site: “local content” with no referer

```
$ curl -L -s 'https://[victim].edu.br/video/2025-05/barcelona%20e%20real%20sociedad' | grep -A2 -i 'page not found'
```

```
<h1 class="list-heading">Page Not Found</h1>
```

```
<h5>Sorry, The page you were looking for could not be found.</h5>
```

```
<p>If you expected this page to exist, you might not have permission to view it.</p>
```

```
</div>
```



# Compromised site:

## “local content” with `www.google.com.br` as the referer

```
$ curl -L -s -e "https://www.google.com.br/" 'https://[victim].edu.br/video/2025-05/barcelona%20e%20real%20sociedad'
<!DOCTYPE html>
[...]  
<script>  
  let countdown = 5;  
  let countdownEl = document.querySelector('.countdown');  
  
  // 进度条动画  
  let progress = 0;  
  let interval = setInterval(() => {  
    progress += 20;  
    document.querySelector('.loader').style.width = progress + '%';  
    if (progress >= 100) {  
      clearInterval(interval);  
    }  
  }, 1000);  
  
  // 倒计时功能  
  let countdownInterval = setInterval(() => {  
    countdown--;  
    countdownEl.textContent = countdown;  
  
    if (countdown <= 0) {  
      clearInterval(countdownInterval);  
      window.location.href = 'https://www.br788cc.com/?ch=12942';  
    }  
  }, 1000);  
  
  // 按钮点击事件, 手动跳转  
  document.getElementById('btn').onclick = () => {  
    window.location.href = 'https://www.br788cc.com/?ch=12942';  
  };  
</script>  
[...]
```

# Challenges

- It is not “one malware”
- Multiple
  - C2s and modules/scripts
  - operating systems
  - webserver
  - setups
- Lack of response from website admins
  - The few that respond are not able to find the root cause of the compromise
    - several remove the modules/scripts, and in 2 or 3 days later are compromised again
- Reports from **international campaigns are different** from the scenario we are seeing in Brazil

# Recommendations to Potential Victims

- Regularly visit your webserver and compare with the Googlebot view

```
$ curl -L -s https://[your_site]/ > normal-view.html
```

```
$ curl -L -s -A Googlebot https://[your_site]/ > googlebot-view.html
```

```
$ diff normal-view.html googlebot-view.html
```

- Enable network **monitoring of outbound traffic**, preferably `netflow`

- Look for connections from webserver to C2 servers
- Identify other servers compromised connecting to the same C2

- To really recover from a compromise, **it is imperative to identify the root cause**

- Was a vulnerability exploited?
  - OS? Webserver? CMS?
- Infostealer at the website admin computer?
- A combination of the above?
- Something else?



# Thank You!

@ Incident reports to: [cert@cert.br](mailto:cert@cert.br) X [@certbr](https://twitter.com/certbr)

<https://cert.br/>

**nic.br** **cgi.br**

[www.nic.br](http://www.nic.br) | [www.cgi.br](http://www.cgi.br)